FOCYM 2026 · OUAGADOUGOU, BURKINA FASO

Un événement fondateur pour la cybersécurité de l'industrie extractive en Afrique de l'Ouest

Pour la première fois en Afrique de l'Ouest francophone, dirigeants miniers, experts en cybersécurité et décideurs institutionnels se réunissent pour faire face ensemble à une menace qui ne connaît pas de frontières.

Informations clés	Détail
Titre de l'événement	Forum International sur la Cybersécurité du Secteur Minier (**FOCYM 2026)**
Organisateur	SKILL CLASS — Abidjan, République de Côte d'Ivoire
Directrice & promotrice	Mme Solange Manuella GBAKA, Directrice du Cabinet SkillClass
Lieu	Ouagadougou, Burkina Faso — Hôtel de prestige
Format	Hybride : présentiel + retransmission en ligne sécurisée
Date	Du 03 au 04 Septembre 2026
Durée	2 jours (8h30 – 18h00)
Public cible	Sociétés minières, institutions publiques, entreprises partenaires
Participants attendus	150 à 180 participants (présentiel & distanciel)
Langues	Français (officiel)
Contact	WhatsApp (+225) 94 19 82 93

I. Contexte et justification

Le secteur minier représente l'un des piliers les plus stratégiques de l'économie burkinabè et de l'Afrique de l'Ouest dans son ensemble. Les exportations minières — or en tête — constituent la principale source de devises pour plusieurs États de la sous-région, alimentant à la fois les budgets nationaux et les projets de développement.

Or, cette industrie vitale est aujourd'hui exposée à une menace d'une nature nouvelle, invisible et souvent sous-estimée : la cybermenace. La transformation numérique accélérée des opérations minières — systèmes de contrôle industriel (SCADA/OT), gestion des données géologiques, plateformes financières dématérialisées, chaînes d'approvisionnement connectées — a considérablement élargi la surface d'attaque des sociétés minières.

Une menace documentée et croissante

Les statistiques mondiales sont sans appel : entre 2020 et 2024, les cyberattaques ciblant le secteur extractif ont progressé de plus de 300 %. Les conséquences sont multiples et graves :

- Arrêts de production forcés liés à des attaques par ransomware, pouvant paralyser une mine pendant plusieurs jours ou semaines
- Exfiltration de données géologiques stratégiques représentant des années de travail d'exploration
- Fraudes financières sophistiquées ciblant les transactions inter-entreprises et les paiements fournisseurs
- Sabotage de systèmes de contrôle industriel pouvant mettre en danger la sécurité physique des travailleurs
- Atteintes à la réputation et perte de confiance des investisseurs et des partenaires

Un retard structurel en Afrique de l'Ouest

En Afrique de l'Ouest, le secteur minier accuse un retard structurel en matière de cybersécurité. Moins de 25 % des sociétés minières actives dans la sous-région disposent d'un Responsable de la Sécurité des Systèmes d'Information (RSSI) à temps plein. Le budget alloué à la cybersécurité représente en moyenne 1,2 % des budgets informatiques, contre 8 à 12 % recommandés par les standards internationaux. Par ailleurs, les cadres réglementaires nationaux sont encore en construction, laissant un vide normatif que les cyberattaquants exploitent.

C'est dans ce contexte que le Cabinet **SkillClass**, fort de son expertise reconnue en formation professionnelle et en développement des capacités en Afrique de l'Ouest, prend l'initiative d'organiser ce forum international — le premier du genre en Afrique francophone dédié exclusivement à la cybersécurité du secteur minier.

II. Objectifs du forum

Le forum poursuit six objectifs stratégiques complémentaires, qui s'articulent depuis la prise de conscience jusqu'à l'action collective et pérenne :

Les 6 objectifs stratégiques du forum		
01	**Sensibiliser**	*Faire prendre conscience aux dirigeants des sociétés minières de la réalité et de la gravité des cybermenaces qui pèsent sur leurs opérations*
02	**Partager**	*Créer un espace d'échange structuré permettant aux praticiens de partager : retours d'expérience, bonnes pratiques et solutions éprouvées*
03	**Former**	*Renforcer les capacités techniques des équipes IT/OT à travers des ateliers pratiques et la simulation live d'une cyberattaque sur infrastructure minière*

04	**Connecter**	*Fédérer les acteurs publics, privés et académiques autour d'une vision commune de la cybersécurité minière en Afrique de l'Ouest*
05	**Recommander**	*Produire un ensemble de recommandations officielles et une déclaration finale adoptée par les participants, transmise aux autorités compétentes*
06	**Pérenniser**	*Jeter les bases d'une coopération régionale durable : ISAC sectoriel, réseau d'experts et engagement vers une 2ème édition*

III. Public cible et participants attendus

Le forum est conçu pour accueillir un public pluridisciplinaire de haut niveau, reflétant la diversité des parties prenantes impliquées dans la cybersécurité du secteur minier :

Profils participants visés	
Dirigeants secteur minier	*DG, DGA, Directeurs Financiers, Directeurs des Opérations des sociétés minières actives au Burkina Faso et en Afrique de l'Ouest*
Responsables IT & Sécurité	*DSI, RSSI, Responsables SI, Administrateurs systèmes et réseaux des sociétés minières*
Représentants institutionnels	*Ministères des Mines et du Numérique, ANPTIC, Chambre des Mines, autorités de régulation*
Experts & Consultants	*Experts en cybersécurité industrielle, consultants OT/SCADA, auditeurs certifiés (CISM, CISSP)*
Partenaires technologiques	*Éditeurs de solutions cybersécurité, fournisseurs d'infrastructure, intégrateurs systèmes*
Acteurs académiques & R&D	*Chercheurs, universités, instituts spécialisés en cybersécurité et en génie minier*

IV. Programme — Aperçu des deux jours

Le programme a été conçu pour alterner formats de haut niveau et sessions opérationnelles, assurant ainsi une valeur ajoutée pour les dirigeants comme pour les praticiens techniques. Il comprend des plénières, des ateliers techniques parallèles, des tables rondes stratégiques et une simulation live de cyberattaque sur infrastructure minière.

JOUR 1 — Ouverture & État des lieux	JOUR 2 — Solutions & Simulation
08h00 : Accueil & enregistrement des participants	**08h30 :** Ouverture Jour 2 & récapitulatif
09h00 : Cérémonie d'ouverture officielle — Allocutions ministérielles	**08h45 :** Architecture de cybersécurité pour une société minière
09h50 : Conférence inaugurale : Le secteur minier, cible prioritaire mondiale	**09h35 :** Gestion de crise cyber : du plan de réponse à la reprise
10h40 : Retour d'expérience : Cybersécurité minière en Afrique de l'Ouest	**10h40 :** Ateliers parallèles : Réseaux · Facteur humain · Innovation
11h40 : Cadre réglementaire et obligations légales des sociétés minières	**12h10 :** Déjeuner & dernière visite exposition
12h20 : Table ronde : Les dirigeants face au risque cyber	**13h30 :** SIMULATION LIVE — « Opération Mine Noire » (2h)
13h00 : Déjeuner officiel & networking	**15h45 :** Table ronde : Coopération régionale et ISAC sectoriel
14h15 : Ateliers parallèles : OT/SCADA · Gouvernance · Data	**16h30 :** Présentation des 10 recommandations officielles
16h00 : Conférence : Anatomie d'une cyberattaque sur mine d'or	**17h00 :** Cérémonie de clôture — Allocutions finales
16h50 : Threat Intelligence et renseignement cyber sectoriel	**17h20 :** Remise attestations & trophées — Photo officielle
17h30 : Synthèse Jour 1 & clôture de séance	**17h40 :** Cocktail de clôture
19h30 : Cocktail de gala VIP	

Temps fort exclusif : *La simulation « Opération Mine Noire » est un exercice de gestion de crise inédit en Afrique francophone. Les participants sont intégrés dans des cellules de crise fictives et doivent répondre en temps réel à une cyberattaque coordonnée frappant simultanément les systèmes SCADA et le SI de gestion d'une mine en activité. Cet exercice constitue une expérience d'apprentissage unique et mémorable.*

V. Valeur ajoutée et résultats attendus

Pour les participants

- Mise à niveau sur les menaces cyber actuelles ciblant spécifiquement le secteur minier
- Acquisition d'outils et de cadres pratiques immédiatement applicables dans leur organisation
- Accès à un réseau d'experts et de pairs de premier plan en Afrique de l'Ouest
- Participation à la simulation live : expérience unique de gestion de crise cyber
- Attestation officielle de participation et accès aux actes du forum

Pour les organisations

- Identification des lacunes de sécurité et des priorités d'investissement
- Mise en conformité accélérée avec les cadres réglementaires en vigueur et à venir

- Visibilité sur les solutions technologiques adaptées au secteur minier africain
- Opportunités de partenariat avec des acteurs institutionnels et des financeurs

Livrables officiels du forum

- Les 10 recommandations officielles adoptées par l'assemblée plénière
- La Déclaration de Ouagadougou sur la cybersécurité minière
- Les actes complets du forum (synthèses, interventions, table ronde)
- Le lancement du groupe de travail ISAC sectoriel minier ouest-africain

VI. Organisation et gouvernance

Organisateur principal

Le Cabinet de formation **SKILL CLASS** est un cabinet de formation et de conseil basé à Abidjan, Côte d'Ivoire, spécialisé dans le développement des compétences professionnelles et le renforcement des capacités organisationnelles en Afrique de l'Ouest. Sous la direction de Madame Solange Manuella GBAKA, le cabinet accompagne depuis plusieurs années des entreprises et des institutions dans leurs parcours de professionnalisation.

Pour ce forum, le Cabinet **SKILL CLASS** s'appuie sur un Comité Scientifique d'experts internationaux en cybersécurité industrielle, un référent opérationnel local à Ouagadougou et un réseau de partenaires institutionnels régionaux.

Une gouvernance scientifique solide

- Comité Scientifique composé d'experts internationaux spécialisés en cybersécurité industrielle (OT/SCADA)
- Référent opérationnel basé à Ouagadougou, garantissant un ancrage local fort
- Réseau de partenaires institutionnels régionaux mobilisés pour la réussite du forum

Format hybride et accessibilité

Le forum adopte un format hybride combinant la richesse des échanges en présentiel à Ouagadougou et l'accessibilité d'une retransmission en ligne sécurisée. Ce choix répond à plusieurs impératifs : maximiser la participation des acteurs régionaux qui ne peuvent pas se déplacer, réduire l'empreinte carbone de l'événement, et créer une communauté numérique durable au-delà des deux jours du forum.

La présente Concept Note est un document de présentation destiné aux partenaires institutionnels, sponsors et participants potentiels du forum. Elle peut être transmise librement sous réserve de mentionner le Cabinet SkillClass comme organisateur. Pour tout renseignement complémentaire, documents détaillés (programme scientifique, budget, dossier de sponsoring, lettres d'invitation), veuillez contacter directement le cabinet.

— SkillClass · Abidjan, Côte d'Ivoire —